

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

Date of mailing (day/month/year)
05 February 2002 (05.02.02)

To:

KLUNKER, SCHMITT-NILSSON, HIRSCH
Winzererstrasse 106
D-80797 München
ALLEMAGNE

Applicant's or agent's file reference
K 54 239/7 JH/ch

IMPORTANT NOTIFICATION

International application No.
PCT/EP00/07597

International filing date (day/month/year)
04 August 2000 (04.08.00)

1. The following indications appeared on record concerning:

the applicant the inventor the agent the common representative

Name and Address

CIFRO GESELLSCHAFT FÜR SICHERHEIT
IN DATENNETZEN MBH IM
GRÜNDUNGSZENTRUM PHYSIK DER LUDWIG-
MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Schellingstrasse 4
D-80799 München
Germany

State of Nationality

DE

State of Residence

DE

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

the person the name the address the nationality the residence

Name and Address

GIESECKE & DEVRIENT GMBH
Prinzregentenstrasse 159
81677 München
Germany

State of Nationality

DE

State of Residence

DE

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:
Assignment.

4. A copy of this notification has been sent to:

the receiving Office
 the International Searching Authority
 the International Preliminary Examining Authority

the designated Offices concerned
 the elected Offices concerned
 other:

Authorized officer

Elisabeth KÖNIG

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Telephone No.: (41-22) 338.83.38

Facsimile No.: (41-22) 740.14.35

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

Date of mailing (day/month/year) 05 February 2002 (05.02.02)
Applicant's or agent's file reference K 54 239/7 JH/ch
International application No. PCT/EP00/07597

From the INTERNATIONAL BUREAU

To:

KLUNKER, SCHMITT-NILSSON, HIRSCH
Winzererstrasse 106
D-80797 München
ALLEMAGNE

IMPORTANT NOTIFICATION

International filing date (day/month/year)
04 August 2000 (04.08.00)

1. The following indications appeared on record concerning:

the applicant the inventor the agent the common representative

Name and Address HAMMONDS Thomas-Wimmer-Ring 17 80539 München Germany	State of Nationality	State of Residence
	Telephone No.	+49 89 207 02 8300
	Facsimile No.	+49 89 207 02 8301
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

the person the name the address the nationality the residence

Name and Address KLUNKER, SCHMITT-NILSSON, HIRSCH Winzererstrasse 106 D-80797 München Germany	State of Nationality	State of Residence
	Telephone No.	089/307-7410
	Facsimile No.	089/307-74141
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned
<input type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned
<input type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:

The International Bureau of WIPO 34, chemin des Colombelettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Elisabeth KÖNIG Telephone No.: (41-22) 338.83.38
---	---

PARTNERSHIP COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION
(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 07 May 2001 (07.05.01)	To: Commissioner US Department of Commerce United States Patent and Trademark Office, PCT 2011 South Clark Place Room CP2/5C24 Arlington, VA 22202 ETATS-UNIS D'AMERIQUE in its capacity as elected Office
International application No. PCT/EP00/07597	Applicant's or agent's file reference VO00A02/P-WO
International filing date (day/month/year) 04 August 2000 (04.08.00)	Priority date (day/month/year) 25 August 1999 (25.08.99)
Applicant VOGEL, Kolja et al	

1. The designated Office is hereby notified of its election made:

in the demand filed with the International Preliminary Examining Authority on:

29 January 2001 (29.01.01)

in a notice effecting later election filed with the International Bureau on:

2. The election was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Peggy Steunenberg Telephone No.: (41-22) 338.83.38
---	---

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

Date of mailing (day/month/year) 23 April 2001 (23.04.01)	To: CIFRO GESELLSCHAFT FÜR SICHERHEIT IN DATENNETZEN MBH IM GRÜNDUNGZENTRUM PHYSIK DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN Schellingstrasse 4 D-80799 München ALLEMAGNE
Applicant's or agent's file reference VO00A02/P-WO	IMPORTANT NOTIFICATION
International application No. PCT/EP00/07597	International filing date (day/month/year) 04 August 2000 (04.08.00)

1. The following indications appeared on record concerning:

the applicant the inventor the agent the common representative

Name and Address KNAUTHE PAUL SCHMITT Prielmayerstrasse 3 80335 München Germany	State of Nationality DE	State of Residence DE
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

the person the name the address the nationality the residence

Name and Address CIFRO GESELLSCHAFT FÜR SICHERHEIT IN DATENNETZEN MBH IM GRUNDUNGZENTRUM PHYSIK DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN Schellingstrasse 4 80799 München Germany	State of Nationality DE	State of Residence DE
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

3. Further observations, if necessary:

The agent in box 1 has renounced his appointment. All further correspondence should now be sent to the applicant, as in box 2.

4. A copy of this notification has been sent to:

<input checked="" type="checkbox"/> the receiving Office	<input checked="" type="checkbox"/> the designated Offices concerned
<input type="checkbox"/> the International Searching Authority	<input type="checkbox"/> the elected Offices concerned
<input type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Ingrid Aulich Telephone No.: (41-22) 338.83.38
---	---

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

Date of mailing (day/month/year) 07 décembre 2001 (07.12.01)	
Applicant's or agent's file reference VO00A02/P-WO	IMPORTANT NOTIFICATION
International application No. PCT/EP00/07597	International filing date (day/month/year) 04 août 2000 (04.08.00)

- 1. The following indications appeared on record concerning:**

the applicant the inventor the agent the common representative

Name and Address	State of Nationality	State of Residence
HAMMONDS Zweibrückenstr. 17 80331 München Germany	Telephone No. +49-89-2 15 79-156	
	Facsimile No. +49-89-2 15 79-157	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

the person the name the address the nationality the residence

Name and Address	State of Nationality	State of Residence
HAMMONDS Thomas-Wimmer-Ring 17 80539 München Germany	Telephone No. +49 89 207 02 8300	
	Facsimile No. +49 89 207 02 8301	
	Teleprinter No.	

- 3. Further observations, if necessary:**

- 4. A copy of this notification has been sent to:**

the receiving Office

the International Searching Authority

the International Preliminary Examining Authority

the designated Offices concerned

the elected Offices concerned

other:

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No.: (41-22) 740.14.35</p>	<p>Authorized officer</p> <p>Elisabeth KÖNIG</p> <p>Telephone No.: (41-22) 338.83.38</p>
---	--

10/049632



23364

PATENT TRADEMARK OFFICE

JC13 Rec'd PCT/PTO 25 FEB 2002

**TRANSLATION OF
ANNEXES
TO IPER
FOR
PCT/EP00/07597**

1. A method for protecting data having an authentication phase with the following steps:
 - (a) providing a biometric feature;
 - (b) digitizing the biometric feature to create digitized biometric authentication feature data;
 - (c) recovering secret data by means of a decryption on the basis of the digitized biometric authentication feature data and on the basis of a coding-theory method.
2. A method according to claim 1 having an initialization phase with the following steps:
 - (a) providing a biometric feature;
 - (b) digitizing the biometric feature to create digitized biometric feature data;
 - (c) providing secret data;
 - (d) encrypting on the basis of the digitized biometric feature data and fault-tolerantly coding the secret data.
3. A method according to claim 2 having the consecutive steps:
 - (a) fault-tolerantly coding the secret data to create a code word;
 - (b) encrypting the code word on the basis of the digitized biometric feature data to create an encrypted code word.
4. A method according to claim 3, wherein the code word is generated by a generating matrix.
5. A method according to claim 2 having the following step: creating initial correction data to describe the space of allowed code words.
6. A method according to claim 1 having the consecutive steps:
 - (a) decrypting the encrypted code word on the basis of the digitized biometric authentication feature data;
 - (b) recovering the secret data on the basis of a coding-theory method.
7. A method according to claim 2 having the following step: providing initialization correction data on the basis of the digitized biometric feature data.
8. A method according to claim 1 having the following steps:

- (a) creating authentication correction data on the basis of the digitized biometric authentication feature data;
 - (b) recovering the digitized biometric feature data on the basis of the authentication and initial correction data;
 - (c) decrypting encrypted secret data on the basis of the recovered digitized biometric feature data.
9. A method according to claim 7, wherein the initial correction data are created by calculation of the digitized biometric feature data modulo n .
 10. A method according to claim 8, wherein the authentication correction data are created by calculation of the authentication feature data modulo n .
 11. A method according to claims 2 to 10 having user-specific initial correction data and/or user-specific fault-tolerant coding.
 12. A method according to any of claims 2 to 11, wherein a public and a secret part are determined or estimated from the biometric feature.
 13. A method according to claim 12, wherein the separation into a public and a secret part of the biometric feature is effected with the aid of empirical inquiries.
 14. A method according to claims 1 to 12, wherein a hash value is created from the digitized biometric feature data with the aid of a hash function.
 15. A method according to any of claims 1 to 14, wherein a hash value is created from the digitized biometric authentication feature data with the aid of a hash function.
 16. A method according to any of the above claims, wherein the biometric feature is a behavioral biometric.
 17. A method according to any of the above claims, wherein the biometric feature consists of a handwritten signature.
 18. A method according to any of the above claims, wherein the handwritten signature is broken down into a public and a secret part and the secret part is a proper subset of the dynamic information of the signature.
 19. A method according to any of the above claims, wherein the providing and/or digitizing of the biometric feature is effected several times.
 20. A method according to any of the above claims, wherein the secret data are generated with a public-key method.

21. An apparatus, in particular for carrying out the method according to any of the above claims, having:
 - (a) means for digitizing a biometric feature to create digitized biometric feature data;
 - (b) means for providing secret data;
 - (c) means for fault-tolerantly coding and decoding the secret data; and
 - (d) means for encrypting and decrypting the secret data with the aid of the digitized biometric feature data.
22. An apparatus according to claim 21 having means for creating code words.
23. An apparatus according to claim 21 having means for creating initial correction data.
24. An apparatus according to any of claims 21 to 23 having means for providing a hash value.
25. An apparatus according to any of claims 21 to 24 having means for breaking down the biometric feature into a public and a secret part.
26. An apparatus according to claim 25 having means for breaking down into a public and a secret part of the biometric feature with the aid of statistical inquiries.
27. An apparatus according to claims 21 to 26 further having means for capturing a handwritten signature as a biometric feature.

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference K 54 239/7 JH/ch	FOR FURTHER ACTION	SeeNotificationofTransmittalofInternational Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP00/07597	International filing date (<i>day/month/year</i>) 04 August 2000 (04.08.00)	Priority date (<i>day/month/year</i>) 25 August 1999 (25.08.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.
<input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
These annexes consist of a total of <u>4</u> sheets.
3. This report contains indications relating to the following items:
I <input checked="" type="checkbox"/> Basis of the report
II <input type="checkbox"/> Priority
III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
IV <input type="checkbox"/> Lack of unity of invention
V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
VI <input type="checkbox"/> Certain documents cited
VII <input checked="" type="checkbox"/> Certain defects in the international application
VIII <input type="checkbox"/> Certain observations on the international application

Date of submission of the demand 29 January 2001 (29.01.01)	Date of completion of this report 28 December 2001 (28.12.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP00/07597

I. Basis of the report

1. With regard to the elements of the international application:*

 the international application as originally filed the description:

pages _____ 1-22 _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

 the claims:

pages _____ 27 _____, as originally filed

pages _____, as amended (together with any statement under Article 19)

pages _____, filed with the demand

pages _____ 1-26 _____, filed with the letter of 13 December 2001 (13.12.2001)

 the drawings:

pages _____ 1/6-6/6 _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

 the sequence listing part of the description:

pages _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

 the language of a translation furnished for the purposes of international search (under Rule 23.1(b)). the language of publication of the international application (under Rule 48.3(b)). the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

 contained in the international application in written form. filed together with the international application in computer readable form. furnished subsequently to this Authority in written form. furnished subsequently to this Authority in computer readable form. The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished. The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.4. The amendments have resulted in the cancellation of: the description, pages _____ the claims, Nos. _____ the drawings, sheets/fig _____5. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

/EP 00/07597

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability: citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	1-26	YES
	Claims		NO
Inventive step (IS)	Claims	1-26	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims		NO

2. Citations and explanations**1. Independent Claims 1 and 20**

The invention relates to a method for protecting data using biometric features (Claim 1) and a device for carrying out this method (Claim 20).

The prior art mentioned in the description discloses methods that guarantee the authenticity and integrity of digitised data using biometric features.

However, these known methods are not open to quantification of protection by biometry.

The problem addressed by the present invention is therefore how to devise a method for protecting data that has a higher level of security than the methods of the prior art and makes quantification of the encryption protection possible by biometry.

The problem is solved by the method steps of Claim 1 and by the device features of Claim 20.

The invention uses a signature method in which the private or secret key (signature key) is encrypted with data that are obtained from a biometric feature

of a private key's owner. For this purpose during the authentication phase a biometric feature is prepared and digitised in a first step. In the next step the signature key (the secret data) is reproduced. Then an encrypted coded word is decrypted using the digitised biometric features and using a coding-theoretical correction method with freely selectable correction capacity.

The international search report citations were already mentioned in the current description as prior art.

The subject matter of Claims 1 and 20 is therefore novel and inventive (PCT Article 33(2) and (3)).

2. Dependent Claims 2 to 19 and 21 to 26

Dependent Claims 2 to 19 and 21 to 26 contain other details of the method and the device according to Claim 1 and Claim 20 respectively. Since they are dependent on Claim 1 and Claim 20 respectively, they also meet the PCT requirements concerning novelty and inventive step (PCT Article 33(2) and (3)).

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP 00/07597

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The features of the claims have not been provided with reference signs in parentheses (PCT Rule 6.2(b)).

VERTRAG ÜBER DIE INTERNATIONALE SAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

REC'D 04 JAN 2002

WIPO PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Annehmers oder Anwalts VO00A02/P-WO	WEITERES VORGEHEN <small>siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)</small>	
Internationales Aktenzeichen PCT/EP00/07597	Internationales Anmeldedatum (Tag/Monat/Jahr) 04/08/2000	Prioritätsdatum (Tag/Monat/Jahr) 25/08/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08		
Annehmer CIFRO GESELLSCHAFT... MBH et al.		

<ol style="list-style-type: none"> 1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Annehmer gemäß Artikel 36 übermittelt. 2. Dieser BERICHT umfasst insgesamt 5 Blätter einschließlich dieses Deckblatts. <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT). <p>Diese Anlagen umfassen insgesamt 4 Blätter.</p>
<ol style="list-style-type: none"> 3. Dieser Bericht enthält Angaben zu folgenden Punkten: <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Grundlage des Berichts II <input type="checkbox"/> Priorität III <input type="checkbox"/> Keine Erstellung eines Gutachtens über Neuheit, erforderliche Tätigkeit und gewerbliche Anwendbarkeit IV <input type="checkbox"/> Mangelnde Einheitlichkeit der Erfindung V <input checked="" type="checkbox"/> Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erforderlichen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung VI <input type="checkbox"/> Bestimmte angeführte Unterlagen VII <input checked="" type="checkbox"/> Bestimmte Mängel der internationalen Anmeldung VIII <input type="checkbox"/> Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 29/01/2001	Datum der Fertigstellung dieses Berichts 28.12.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Apostolescu, R Tel. Nr. +49 89 2399 7950

**INTERNATIONALER VORLÄUFIGER
PRÜFUNGSBERICHT**

Internationales Aktenzeichen PCT/EP00/07597

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-22 ursprüngliche Fassung

Patentansprüche, Nr.:

27 ursprüngliche Fassung

1-26 mit Telefax vom 13/12/2001

Zeichnungen, Blätter:

1/6-6/6 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

**INTERNATIONALER VORLÄUFIGER
PRÜFUNGSBERICHT**

Internationales Aktenzeichen PCT/EP00/07597

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- Beschreibung, Seiten:
 Ansprüche, Nr.:
 Zeichnungen, Blatt:

5. Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N) Ja: Ansprüche 1-26
Nein: Ansprüche

Erfinderische Tätigkeit (ET) Ja: Ansprüche 1-26
Nein: Ansprüche

Gewerbliche Anwendbarkeit (GA) Ja: Ansprüche 1-26
Nein: Ansprüche

2. Unterlagen und Erklärungen
siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Unabhängige Ansprüche 1 und 20.

Die Erfindung bezieht sich auf ein Verfahren zum Schutz von Daten anhand biometrischer Merkmale (Anspruch 1) und eine Vorrichtung zur Durchführung dieses Verfahrens (Anspruch 20).

Aus dem in der Beschreibung genannten Stand der Technik sind Verfahren bekannt, die die Authentizität und Integrität von digitalisierten Daten anhand biometrischer Merkmale gewährleisten.

Diese bekannten Verfahren sind jedoch einer Quantifizierung des Schutzes durch Biometrie nicht zugänglich.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Schutz von Daten zu schaffen, dass eine gegenüber den Verfahren der Technik erhöhte Sicherheit aufweist und dass eine Quantifizierung des Verschlüsselungsschutzes durch Biometrie ermöglicht.

Gelöst wird die Aufgabe durch die Vefahrensschritte des Anspruchs 1 sowie durch die Vorrichtungsmerkmale des Anspruchs 20.

Die Erfindung verwendet ein Signaturverfahren, bei dem der private bzw. geheime Schlüssel (Signaturschlüssel) mit Daten verschlüsselt wird, die aus einem biometrischen Merkmal des Besitzers des privaten Schlüssels gewonnen werden. Dazu wird in einem ersten Schritt in der Authentifizierungsphase ein biometrisches Merkmal bereitgestellt und digitalisiert. In einem nächsten Schritt wird der Signaturschlüssel (die geheimen Daten) wiederhergestellt. Dazu wird ein verschlüsseltes Kodewort anhand der digitalisierten biometrischen Merkmale und anhand eines kodierungstheoretischen Korrekturverfahrens mit frei wählbaren Korrekturkapazität entschlüsselt.

Die im Internationalen Recherchenbericht genannten Druckschriften waren auch bereits in der vorliegenden Beschreibung als Stand der Technik angegeben.

Der Gegenstand der Ansprüche 1 und 20 ist daher neu und erfinderisch (Artikel 33 (2) und (3) PCT).

2. Abhängige Ansprüche 2 bis 19 und 21 bis 26.

Die abhängigen Ansprüche 2 bis 19 und 21 bis 26 enthalten weitere Details des Verfahrens und der Vorrichtung gemäß Anspruch 1 bzw. 20. Da sie vom Anspruch 1 bzw. 20 abhängig sind, erfüllen auch sie die Erfordernisse gemäß PCT (Artikel 33 (2) und (3)) bezüglich Neuheit und erfinderischer Tätigkeit.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

Die Merkmale der Ansprüche sind nicht mit in Klammern gesetzten Bezugszeichen versehen worden (Regel 6.2 b) PCT).

Patentansprüche

1. Verfahren zum Schutz von Daten, das eine Authentifizierungsphase mit folgenden Schritten aufweist:
 - (a) Bereitstellung eines biometrischen Merkmals;
 - (b) Digitalisierung des biometrischen Merkmals zur Erstellung von digitalisierten biometrischen Authentifizierungsmerkmalsdaten; gekennzeichnet durch
 - (c) Entschlüsselung eines verschlüsselten Kodewortes anhand der digitalisierten biometrischen Authentifizierungsmerkmalsdaten;
 - (d) Wiederherstellung geheimer Daten mittels einer Entschlüsselung des Kodewortes anhand der digitalisierten biometrischen Authentifizierungsmerkmalsdaten und anhand eines kodierungstheoretischen Korrekturverfahrens mit Korrekturkapazität, wobei die Korrekturkapazität frei wählbar ist.
2. Verfahren nach Anspruch 1, das eine Initialisierungsphase mit folgenden Schritten aufweist:
 - (a) Bereitstellung eines biometrischen Merkmals;
 - (b) Digitalisierung des biometrischen Merkmals zur Erstellung von digitalisierten biometrischen Merkmalsdaten;
 - (c) Bereitstellung von geheimen Daten;
 - (d) Verschlüsselung anhand der digitalisierten biometrischen Merkmalsdaten und fehlertolerante Kodierung der geheimen Daten.
3. Verfahren nach Anspruch 2, das die auf einander folgenden Schritte aufweist:
 - (a) Fehlertolerante Kodierung der geheimen Daten zur Erstellung eines Kodeworts;
 - (b) Verschlüsselung des Kodeworts anhand der digitalisierten biometrischen Merkmalsdaten zur Erstellung eines verschlüsselten Kodeworts.

4. Verfahren nach Anspruch 3, wobei das Kodewort durch eine generierende Matrix erzeugt wird.
5. Verfahren nach Anspruch 2, das den folgenden Schritt aufweist: Erstellung von Initial-Korrekturdaten zur Beschreibung des Raums erlaubter Kodeworte.
6. Verfahren nach Anspruch 2, das den folgenden Schritt aufweist: Bereitstellung von Initialisierungs-Korrekturdaten anhand der digitalisierten biometrischen Merkmalsdaten.
7. Verfahren nach Anspruch 1, das folgende Schritte aufweist:
 - (a) Erstellung von Authentifizierungs-Korrekturdaten anhand der digitalisierten biometrischen Authentifizierungsmerkmalsdaten;
 - (b) Wiederherstellung der digitalisierten biometrischen Merkmalsdaten anhand der Authentifizierungs- und Initial-Korrekturdaten;
 - (c) Entschlüsselung verschlüsselter geheimer Daten anhand der wiederhergestellten digitalisierten biometrischen Merkmalsdaten.
8. Verfahren nach Anspruch 6, wobei die Initial-Korrekturdaten durch Berechnung der digitalisierten biometrischen Merkmalsdaten modulo n erstellt werden.
9. Verfahren nach Anspruch 7, wobei die Authentifizierungs-Korrekturdaten durch Berechnung der Authentifizierungsmerkmalsdaten modulo n erstellt werden.
10. Verfahren nach Anspruch 2 bis 9, das benutzerspezifische Initial-Korrekturdaten und/oder benutzerspezifische fehlertolerante Kodierung aufweist.
11. Verfahren nach einem der Ansprüche 2 bis 10, bei dem aus dem biometrischen Merkmal ein öffentlicher und ein geheimer Teil bestimmt oder geschätzt wird.

VO00A02/R

12. Verfahren nach Anspruch 11, bei dem die Trennung in einen öffentlichen und einen geheimen Teil des biometrischen Merkmals mit Hilfe von empirischen Erhebungen erfolgt.
13. Verfahren nach Anspruch 1 bis 11, bei dem mit Hilfe einer Hash-Funktion aus den digitalisierten biometrischen Merkmalsdaten ein Hash- Wert erstellt wird.
14. Verfahren nach einem der Ansprüche 1 bis 13, bei dem mit Hilfe einer Hash-Funktion aus den digitalisierten biometrischen Authentifizierungs-Merkmalen ein Hash-Wert erstellt wird.
15. Verfahren nach einem der vorhergehenden Ansprüche, bei dem das biometrischen Merkmal eine Verhaltensbiometrie ist.
16. Verfahren nach einem der vorhergehenden Ansprüche, bei dem das biometrische Merkmal aus einer handschriftlich geleiteten Unterschrift besteht.
17. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die handschriftlich geleistete Unterschrift in einen öffentlichen und einen geheimen Teil zerlegt wird und der geheime Teil eine echte Untergruppe der dynamischen Information der Unterschrift ist.
18. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Bereitstellung und/oder Digitalisierung des biometrischen Merkmals mehrfach erfolgt.
19. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die geheimen Daten mit einem Public-Key- Verfahren erzeugt werden.
20. Vorrichtung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche mit:
 - (a) einem Mittel zur Digitalisierung eines biometrischen Merkmals zur Erstellung von digitalisierten biometrischen Merkmalsdaten;

- (b) einem Mittel zur Bereitstellung von geheimen Daten; gekennzeichnet durch
- (c) ein Mittel zur fehlertoleranten Kodierung und zur Dekodierung der geheimen Daten; sowie
- (d) ein Mittel zur Ver- und Entschlüsselung der fehlertolerant kodierten geheimen Daten mit Hilfe der digitalisierten biometrischen Merkmalsdaten.
21. Vorrichtung nach Anspruch 20, die ein Mittel zur Erstellung von Kodeworten aufweist.
22. Vorrichtung nach Anspruch 20, die ein Mittel zur Erstellung von Initial-Korrekturdaten aufweist.
23. Vorrichtung nach einem der Ansprüche 20 bis 22, die ein Mittel zur Bereitstellung eines Hashwerts aufweist.
24. Vorrichtung nach einem der Ansprüche 20 bis 23, die ein Mittel zur Zerlegung des biometrischen Merkmals in einen öffentlichen und einen geheimen Teil aufweist.
25. Vorrichtung nach Anspruch 24, die ein Mittel zur Zerlegung in einen öffentlichen und einen geheimen Teil des biometrischen Merkmals mit Hilfe von statistischen Erhebungen aufweist.
26. Vorrichtung nach Anspruch 20 bis 25, die ferner ein Mittel zur Erfassung einer handschriftlich geleisteten Unterschrift als biometrisches Merkmal aufweist.

1.20
VERTRÄG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTENESSENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts V000A02/P-W0	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 00/07597	Internationales Anmeldedatum (Tag/Monat/Jahr) 04/08/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 25/08/1999
Anmelder CIFRO GESELLSCHAFT... MBH		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
- Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.
- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das
- in der internationalen Anmeldung in Schriftlicher Form enthalten ist.
- zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung

- wird der vom Anmelder eingereichte Wortlaut genehmigt.
- wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung

- wird der vom Anmelder eingereichte Wortlaut genehmigt.
- wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 7

- wie vom Anmelder vorgeschlagen
- weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
- weil diese Abbildung die Erfindung besser kennzeichnet.
- keine der Abb.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/07597

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 IPK 7 H04L9/08 H04L9/32 G06K9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 IPK 7 G07C G06K H03M H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 42 43 908 A (GAO GES AUTOMATION ORG) 30. Juni 1994 (1994-06-30) in der Anmeldung erwähnt Zusammenfassung; Abbildungen Spalte 3, Zeile 20 -Spalte 5, Zeile 54	1, 6, 15, 16, 20-22, 24
Y	---	2-5, 7, 9, 17, 19, 23, 27
X	WO 99 33219 A (KONINKL PHILIPS ELECTRONICS NV ;PHILIPS AB (SE)) 1. Juli 1999 (1999-07-01) Zusammenfassung; Abbildung 1 Seite 6, Zeile 18 -Seite 7, Zeile 34 ----	1, 15, 16, 20-22, 24

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

- * Besondere Kategorien von angegebenen Veröffentlichungen :
- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldeatum veröffentlicht worden ist
- *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- *P* Veröffentlichung, die vor dem internationalen Anmeldeatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
- *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldeatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
- *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
- *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
- *&* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
4. Dezember 2000	21/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Buron, E
---	---

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/07597

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 98 52317 A (VERIDICOM INC) 19. November 1998 (1998-11-19) in der Anmeldung erwähnt Zusammenfassung; Abbildungen 1,2,5 Seite 4, Zeile 16 -Seite 6, Zeile 2 Seite 12, Zeile 6 - Zeile 16 Seite 14, Zeile 7 -Seite 15, Zeile 23 ---	1,16,17, 21
Y	DAVIDA, FRANKEL,MATT: "On enabling secure applications through off-line biometric identification" 1998 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 3. - 6. Mai 1998, XP002154556 Oakland USA Absatz '03.2! - Absatz '05.1! Absatz '05.2! ---	2-5,7,9, 19,23
Y	EP 0 867 827 A (CADIX INC) 30. September 1998 (1998-09-30) Zusammenfassung; Abbildung 1 ---	17,27
A	US 5 228 094 A (VILLA PIERRE) 13. Juli 1993 (1993-07-13) ---	
A	US 5 708 667 A (HAYASHI TOMOHIRO) 13. Januar 1998 (1998-01-13) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/07597

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
DE 4243908	A	30-06-1994	NONE			
WO 9933219	A	01-07-1999	AU EP	1348799 A 0965200 A		12-07-1999 22-12-1999
WO 9852317	A	19-11-1998	US AU EP	5991408 A 7379798 A 0983662 A		23-11-1999 08-12-1998 08-03-2000
EP 0867827	A	30-09-1998	JP	10261082 A		29-09-1998
US 5228094	A	13-07-1993	FR DE DE EP	2671210 A 69110648 D 69110648 T 0493243 A		03-07-1992 27-07-1995 01-02-1996 01-07-1992
US 5708667	A	13-01-1998	JP JP	2905368 B 7056757 A		14-06-1999 03-03-1995